



Legislative Audit Division

State of Montana

Report to the Legislature

February 2006

Information System Audit

Montana Lottery Security

Department of Administration

This report contains information regarding the security controls over Montana Lottery operations as required by section 23-7-411, MCA. The report contains nine findings and recommendations addressing the statutory areas of personnel security, contractor security, computer security, data communications security, systems security, and lottery premises and warehouse security.

**Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705**

06DP-03

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Joe Balyeat, Vice Chair
Senator John Brueggeman
Senator Jim Elliott
Senator Dan Harrington
Senator Lynda Moss
Senator Corey Stapleton

Representative Dee Brown
Representative Hal Jacobson
Representative Christine Kaufmann
Representative Scott Mendenhall
Representative John Musgrove, Chair
Representative Janna Taylor

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel



Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

February 2006

The Legislative Audit Committee
of the Montana State Legislature:

This is the report of our security audit over the operation of the Montana Lottery. The report concludes that overall, Lottery security controls are in place in the areas outlined in statute, but the implementation of controls can be improved to adhere to written internal policies and Multi-State Lottery Association rules. The report contains nine recommendations and the Lottery response to the audit report is contained at the end of the report.

We wish to express our appreciation to the staff of the Lottery for their cooperation and assistance.

Respectfully submitted,

A blue ink signature of Scott A. Seacat, written in a cursive style.

Scott A. Seacat
Legislative Auditor

Legislative Audit Division

Information System Audit

Montana Lottery Security

Department of Administration

Members of the audit staff involved in this audit were David P. Nowacki, Dale Stout, and Nathan Tobin.

Table of Contents

Appointed and Administrative Officials	ii
Executive Summary	S-1
Chapter I - Introduction and Background	1
Introduction.....	1
Objectives	1
Scope and Methodology	2
Prior Audit Recommendations.....	3
Conclusion	3
Chapter II - Findings and Recommendations	5
Introduction.....	5
Game Management System and Database Access Not Reviewed	5
Computer Gaming System Secondary System Operation	6
Data Communications Security	7
Review of Firewall Configurations	7
Systems Security.....	7
Internal Control System Accounts Not Managed Properly	8
Internal Control System Maintenance Not Documented	9
Patch Management.....	9
Desktop Patches Missing.....	10
Remote Access Software Patches Missing.....	10
Database Software Out of Date	10
Personnel and Contractor Security	11
Security of Lottery Premises and Warehouse	12
Visitor Logs	13
Lottery Headquarter and Warehouse Visitor Logs are Not Complete.....	13
Electronic Access to Lottery Premises	13
Key Card Access for Contractors Not Controlled	14
Montana Lottery Response	A-3

Appointed and Administrative Officials

Montana Lottery Commission

Robert Crippen, Chair	Butte
Craig Anderson, Sheriff	Glendive
Thomas M. Keegan	Helena
Betty Wilkins	Missoula
Wilbur Rehmann	Helena

Department of Administration

Janet Kelly, Director

Montana Lottery

George Parisot, Montana Lottery Director

John Tarr, Director of Security

Paul Gilbert, Information Systems Director

Executive Summary

State law requires the Legislative Audit Division to conduct a comprehensive audit of the Montana Lottery (Lottery) security every two years. Our primary objective is to evaluate the existence and operation of security controls and evaluate compliance regarding the areas specifically outlined in section 23-7-411, MCA.

The Lottery is a member of the Multi-State Lottery Association (MUSL), a non-profit, government-benefit association owned and operated by its member lotteries. MUSL rules require the Lottery to operate a computer gaming system to manage both online and instant games, and operate an internal control system as a check and balance for online drawings. The Lottery depends on a contractor and subcontractor to maintain these systems. In March 2006, the Lottery's current contract will expire, and a new contractor will implement and maintain a new computer gaming system and internal control system.

Audit scope included evaluating the Lottery against MUSL regulations, Montana Lottery internal security procedures, statewide information technology policies, and information technology industry standard practices in the areas outlined in statute. To ensure our primary objective was met, we observed daily operations, interviewed key Lottery staff, conducted walkthroughs of facilities, and confirmed that documentation was maintained to demonstrate established procedures were being followed. We reviewed computer systems and network configurations through observation and the use of audit software tools to determine adequate security access controls are present.

Overall, security controls are in place in the areas outlined in statute. However, the implementation of controls can be improved to adhere to written internal policies and MUSL rules. We confirmed the implementation status of our nine prior audit recommendations. Seven recommendations were implemented, and two were partially implemented. This report discusses nine findings and recommendations addressing the statutory areas of personnel security, contractor security, computer security, data

Executive Summary

communications security, systems security, and lottery premises and warehouse security.

Chapter I - Introduction and Background

Introduction

The Montana Lottery (Lottery) was created in 1987. The Lottery's operations are entirely funded by the sale of lottery tickets. Lottery games consist of two primary categories, scratch and online games. Scratch tickets are also known as instant tickets because the tickets contain predetermined winners that can be validated instantly at a lottery retailer. Players identify winners by following directions on game tickets and scratching the latex coating off the play area of a ticket to win the prizes associated with the ticket. Online game tickets are issued at lottery retailers via online lottery terminals. Winners are determined through biweekly drawings. Net profits from the sale of tickets are transferred into the state of Montana's General Fund. In fiscal year 2005, approximately \$6.2 million was transferred into the General Fund.

The Lottery is a member of the Multi-State Lottery Association (MUSL), a non-profit, government-benefit association owned and operated by its member lotteries. Each MUSL member offers one or more of the games administered by MUSL. All profits are retained by the individual lotteries and are used to fund projects approved by the legislature authorizing each lottery. MUSL rules require the Lottery to operate a computer gaming system to manage both online and instant games, and operate an internal control system as a check and balance for online drawings. The Lottery depends on a contractor and subcontractor to maintain these systems, and the contractor also provides a game management system to aid Lottery in managing instant ticket games and inventory. In March 2006, the Lottery's current contract will expire, and a new contractor will implement and maintain a new computer gaming system and internal control system. As part of our statutory duties, the Legislative Audit Division will monitor the implementation of the new system, and review changes made to the system that impact security.

Objectives

State law requires the Legislative Audit Division to conduct a comprehensive audit of the Montana Lottery security every two years. Our primary objective is to evaluate the existence and

Chapter I - Introduction and Background

operation of security controls and evaluate compliance regarding the areas specifically outlined in section 23-7-411, MCA:

- a) personnel security;
- b) lottery sales agent security;
- c) lottery contractor security;
- d) security of manufacturing operations of lottery contractors;
- e) security against ticket or chance counterfeiting and alteration and other means of fraudulently winning;
- f) security of drawings among entries or finalists;
- g) computer security;
- h) data communications security;
- i) database security;
- j) systems security;
- k) lottery premises and warehouse security;
- l) security in distribution;
- m) security involving validation and payment procedures;
- n) security involving unclaimed prizes;
- o) security aspects applicable to each particular lottery game;
- p) security of drawings in games whenever winners are determined by drawings;
- q) the completeness of security against locating winners in lottery games with preprinted winners by persons involved in their production, storage, distribution, administration, or sales; and
- r) any other aspects of security applicable to any particular lottery game and to the lottery and its operations.

Scope and Methodology

Audit scope included evaluating the Lottery against Multi-State Lottery Association (MUSL) regulations, Montana Lottery internal security procedures, statewide information technology policies, and information technology industry standard practices in the areas outlined in statute. We also confirmed the implementation status of our nine prior audit recommendations. To ensure our primary objective was met, we observed daily operations, interviewed key Lottery staff, and confirmed that documentation was maintained to demonstrate established procedures were being followed. We

Chapter I - Introduction and Background

reviewed employee and contractor security files for adherence to internal security investigation procedures, which can include background checks or credit checks. We reviewed employee and contractor access to facilities, systems, and data to determine the principle of least privilege is being followed. The principle of least privilege involves giving personnel no more privilege than is necessary to perform a job. Ensuring least privilege requires identifying what the job is, determining the minimum set of privileges required to perform that job, and restricting personnel to a level with those privileges and nothing more. We observed instant ticket stock distribution procedures and identified controls to deter ticket fraud. We reviewed physical security controls over the Lottery premises, warehouse and systems contractor facilities. We reviewed computer systems and network configurations through observation and the use of audit software tools to determine adequate security access controls are present. This audit was conducted in accordance with government auditing standards published by the United States Government Accountability Office.

Prior Audit Recommendations

Our previous audit report (Montana Lottery Security, 03DP-03) contained nine recommendations. Through interviews of key Lottery personnel, observation, and documentation review, we determined the Lottery implemented seven of the nine the recommendations. Two recommendations were partially implemented. Recommendation #6 stated that the Lottery “Change the administrator account default username, and change the password on the administrator account in accordance with state policy,” and Recommendation #8 stated that the Lottery “Ensure credit and criminal inquiries are performed and documentation exists for owners of the external accounting firm and owners of the janitorial services company.” These issues are further discussed in Chapter II of this report.

Conclusion

Overall, security controls are in place in the areas outlined in statute. However, the implementation of controls can be improved to adhere to written internal policies and MUSL rules. Awareness of MUSL requirements by the Lottery and contractor staff was not

Chapter I - Introduction and Background

comprehensive. The following chapter discusses nine findings and recommendations addressing the statutory areas of personnel security, contractor security, computer security, data communications security, systems security, and lottery premises and warehouse security. In accordance with section 23-7-412, MCA, some of the audit finding specific details could compromise security, and therefore are not fully disclosed in this report.

Chapter II - Findings and Recommendations

Introduction

The Lottery has established an internal Security Procedures Manual, which outlines procedures used to fulfill statutory areas as well as MUSL rules. There are three primary systems involved in the operation of the Lottery. The computer gaming system operates both online and instant games, the internal control system operates as a check and balance and reconciliation to the computer gaming system for drawings, and the game management system is also used by the Lottery to manage instant games and inventories. This report contains nine findings and recommendations encompassing personnel security, contractor security, computer security, data communications security, systems security, and lottery premises and warehouse security.

Game Management System and Database Access Not Reviewed

MUSL standards state “all access permissions for operators of the gaming system application and the operating system that it resides on are to be kept to a minimum and shall be granted based on a ‘least privilege’ security model.” We reviewed access to the game management system for all users, and identified contractors with excessive access privileges to the system. We determined contractors all use one default administrative account to the system, allowing full privilege levels. This level of access is not necessary for all of the contractor personnel to perform their responsibilities, and does not follow the model of least privilege. For example, some operators only need the ability to perform back-ups of the system, but because they use the administrative account, they have access privileges that they shouldn’t, such as the ability to change information on the system. Unauthorized changes could be made without any individual accountability or audit trail.

The use of the default user account name presents a risk known in the hacker community, and unauthorized users could target and compromise that account, gaining full access to the system. Lottery personnel stated they do not have procedures in place to periodically review access privileges of contractors for the computer gaming system and the game management system. By not reviewing access privileges for all users, Lottery cannot ensure that users have the

Chapter II - Findings and Recommendations

least access necessary for their job, and the potential exists that users could make unauthorized changes to the system.

Recommendation #1

We recommend the Lottery:

- A. Discontinue the use of the default administrative account.**
- B. Comply with MUSL standards and ensure the ‘least privilege’ security model is followed for the computer gaming system and game management system.**
- C. Establish procedures to periodically review contractor access privileges.**

Computer Gaming System Secondary System Operation

While reviewing the computer gaming system security, we determined that the secondary system, or back-up system, was not run as the primary system for a minimum of one draw period on a semi-annual schedule as required by MUSL standards. This procedure is important to ensure that the secondary system can operate in the primary system’s absence for a prolonged period of time if a major failure occurs to the primary system. The contractor who maintains the computer gaming system was unaware of the requirement. Lottery personnel stated that they don’t ensure their contractors are compliant with MUSL standards. The MUSL requirement is not met and the Lottery cannot be sure that the secondary system can run as a back-up for one full draw period. The contract for the new system, effective March 2006, contains more specific language regarding awareness of and compliance with MUSL standards and state of Montana information technology policies and standards.

Recommendation #2

We recommend the Lottery:

- A. Comply with MUSL requirements to run the secondary computer gaming system as the primary computer gaming system during a minimum of one draw period on a semi-annual schedule.**
- B. Ensure contractors are aware of MUSL requirements.**

Chapter II - Findings and Recommendations

Data Communications Security

To ensure data communications security in accordance with section 23-7-411(h), MCA, the Lottery has implemented a firewall to isolate its network and the internal control system from the rest of the state network.

Review of Firewall Configurations

MUSL standards require firewall and other access control device configurations to be reviewed by the Lottery on a semi-annual basis and whenever changes are made. During our review of the firewalls for the internal control system, we determined Lottery is not reviewing firewall configurations semi-annually. Lottery relies on Department of Administration, Information Technology Services Division (ITSD) personnel to perform maintenance and changes to the firewalls, but the Lottery does not have a control in place to detect unauthorized changes to the firewall. Lottery personnel stated that staff do not have the technical knowledge necessary to perform the reviews, and that the amount of training required to gain this knowledge would be significant. Changes made to firewall configurations can significantly impact the operation of systems because unnecessary traffic could be allowed to communicate with the system, which could open a path for vulnerabilities such as worms, viruses, or intruders. The Lottery needs to ensure the biannual reviews are performed, either through acquiring the necessary training to provide the technical knowledge to perform the review internally, or a written service agreement to have the reviews performed.

Recommendation #3

We recommend the Lottery comply with MUSL standards to review firewall configurations on a semi-annual basis.

Systems Security

We evaluated security controls over the three systems against MUSL standards, as well as information technology industry standard practices, to determine that the Lottery ensures systems security in accordance with section 23-7-411(j), MCA.

Chapter II - Findings and Recommendations

Internal Control System Accounts Not Managed Properly

The Lottery network security plan states that passwords for the internal control system must be changed every sixty days. While reviewing the system user and account maintenance procedures for the internal control system, we determined Lottery is not requiring users to change their passwords every sixty days, although the system functionality is available. Lottery personnel stated that because there are a limited number of users to the internal control system, and that access to the system is also limited by physical controls, the risk is low. However, the Lottery recognized the importance of this security control, and documented it as a control in its written security plan.

MUSL standards also state that “logical access permissions to the both the primary and secondary internal control systems be kept to a minimum.” The Lottery currently allows the internal control system contractor two access accounts, which is greater than the amount needed to regularly maintain the system. Lottery personnel stated the additional account was created for a specific circumstance, but is not needed regularly. Because the account is not needed regularly, the use of it on a routine basis presents a risk that unauthorized changes could be made to the system.

The Lottery is not in compliance with its written network security plan, and not changing the passwords regularly increases the likelihood that a password can be compromised, which would allow unauthorized access to the system. Additionally, the Lottery is not in compliance with statewide information technology policy ENT-SEC-063, which states that passwords will be changed at least every sixty days, or the MUSL standard that states the logical access to the internal control system be kept to a minimum.

Recommendation #4

We recommend the Lottery:

- A. Comply with password change policies to change passwords every sixty days.**
- B. Eliminate all but one contractor internal control system account.**

Chapter II - Findings and Recommendations

Internal Control System Maintenance Not Documented

MUSL standards state that in the event internal control system vendors indicate to the Lottery that they require access to the system, the Lottery shall require the vendor to submit a written request that explains the need for access, the level of access required, and the specific changes to be made. The Lottery currently does not require the contractor to submit written requests as most requests are submitted over the phone. Lottery personnel stated that they have a level of trust with the vendor, and do not believe a formal procedure is necessary. The Lottery has not acknowledged or recognized the risks associated with permitting access requests over the phone, which include lack of individual accountability, and lack of a change control trail. Further, in March of 2006, a new contractor will be maintaining the internal control system, and the Lottery will not be familiar with the personnel and will not have the same level of trust. These requests should not be submitted over the phone, but in writing.

MUSL standards also state “records of operating system and application maintenance or revision to the internal control system shall be thoroughly documented and maintained.” The Lottery does not currently maintain documentation on changes made to the system, including essential change management documentation such as an authorization for changes to be made. Although the Lottery does maintain a physical log of contractors that access the system, the log does not document system maintenance and revisions.

Recommendation #5

We recommend the Lottery comply with MUSL standards to ensure contractor access requests and maintenance and changes to the internal control system are documented.

Patch Management

To ensure computer security in accordance with section 23-7-411(g), MCA, the Lottery is responsible for ensuring software and hardware are kept up to date with patches. Patch management is important because software vendors release updates and patches to correct errors and security vulnerabilities. By not ensuring software patches

Chapter II - Findings and Recommendations

are current, the Lottery is potentially open to vulnerabilities such as viruses and worms.

Desktop Patches Missing

Using electronic audit software, we scanned desktop computers at Lottery headquarters to confirm whether they were current with the latest patches and updates. Of the twenty-three desktops scanned, fifteen were missing the latest patches. One was missing as many as twenty-four patches, and another was missing twenty-five patches. Lottery personnel responded that the two machines weren't patched because they had been recently rebuilt, and personnel had forgotten to patch them, while the remaining were waiting to be tested because the patches were released within the last week. When we notified them of the security risks, Lottery personnel patched the two machines that were missing an excessive amount of patches, and stated that the remaining would be patched at the beginning of 2006. The remaining had not been patched at the time of our audit. Montana Enterprise IT policy ENT-SEC-112 states, "all workstations, portable computers, and PDA's must be updated with the latest security patches, virus scanning software and virus data files. Agencies are responsible for installing the patches, virus scanning software and virus data files on their devices." ITSD has an automated update service available for the updating and patching desktop operating systems, but the Lottery currently depends on a manual process to update each machine individually.

Remote Access Software Patches Missing

While reviewing the contractor internal control system maintenance operations, we determined the remote access software used by the Lottery to allow the contractor access to the internal control system was out of date. Lottery personnel stated they were unaware that patches and updates existed for the software, and the contractor recommended the version they were using.

Database Software Out of Date

While reviewing patching operations performed by the contractor responsible for the computer gaming system, the contractor stated the database version they are using was current. When we checked the database vendor's website to verify, we determined the database version used in the computer gaming system is four versions old, and

Chapter II - Findings and Recommendations

is no longer supported by the vendor. Lottery personnel stated they do not currently have procedures to review and monitor versions of the software used by the contractor in operating the computer gaming system, and were unaware of the out of date software.

The Lottery needs to stay informed of vendors' security-related updates to its products by periodically visiting websites or signing up to receive update notifications. When an update is released, the Lottery should evaluate it to determine its applicability prior to installing it. The Lottery is not currently informed of newly released software updates for contractor software, and does not ensure desktops under the control of the Lottery are patched in accordance with statewide IT policy.

Recommendation #6

We recommend the Lottery:

- A. Establish patch management procedures for the systems under its operation, including the computer gaming system and internal control system.**
- B. Ensure desktop machines are patched in accordance with statewide IT policy.**

Personnel and Contractor Security

To ensure personnel and contractor security operates in accordance with section 23-7-411(a)(c), MCA, Lottery has documented procedures established to maintain a security file for all new employees as well as contractors. The employee and contractor security files contain documentation to demonstrate compliance with various investigation and security orientation procedures outlined in the Security Procedures Manual.

The Lottery is not following established procedures to conduct investigations for all new employees and contractors. We reviewed thirty-five employee files for compliance with security investigation and orientation procedures. We identified missing documentation in ten of the files. Three new employees did not have a security file, and other missing documentation included background checks, new employee security checklists, and security authorization to release

Chapter II - Findings and Recommendations

information. We also reviewed files for the four new contractors that the Lottery has established contracts with since our prior audit (03DP-03). The Lottery Security Procedures Manual states “All firms and individuals seeking to provide goods and services to the Montana Lottery will be subjected to an investigation to determine their suitability.” Of the four new contractors, two did not have files established, which would contain documentation supporting the investigations. The contractors were a general equipment maintenance firm and a marketing firm. Lottery security personnel responded that background checks were not performed for either firm, and believed that the risk was low because personnel are always monitored when they are at the headquarters. However, the Lottery recognized the risk enough to also include in the procedures the statement: “A contractor seeking to provide general products/services, (i.e. janitorial, etc) will include Montana Criminal History inquiry, and credit history of the owners of the firm.” By not maintaining the appropriate documentation, the Lottery cannot effectively demonstrate compliance with established employee and contractor security procedures. Current practice conflicts with formal documented procedures. The Lottery depends upon its investigation procedures to maintain the integrity of personnel and contractors involved in its operations, by not following these procedures for all employees and contractors, the integrity of Lottery operations may be compromised.

Recommendation #7

We recommend the Lottery comply with internal security investigation procedures and ensure files for all employees and contractors are maintained, containing necessary documentation.

Security of Lottery Premises and Warehouse

To ensure security of the Lottery premises and warehouse, in accordance with section 23-7-411(k), MCA, Lottery has documented procedures in the Lottery Security Procedures Manual. Outlined in those procedures are visitor procedures, physical monitoring of visitor areas, electronic key card access, and alarm systems that include motion detectors.

Chapter II - Findings and Recommendations

Visitor Logs

The Lottery has documented procedures established to maintain physical logs of all visitors to the Lottery Headquarters and Warehouse. The Lottery headquarters log contains columns for date, time-in, time-out, name, firm represented, visitor badge number, and person visited. The warehouse log has columns for date, entry and exit time, reason for entry, and name.

Lottery Headquarter and Warehouse Visitor Logs are Not Complete

The Lottery is not following established procedures to ensure the completeness of visitor logs. We reviewed visitor logs for the Lottery Headquarters from December 2004 to November 2005. Of the 396 entries reviewed, 171 were missing accountability indicators such as name, firm represented, and person visiting, 13 did not include time-in, 94 did not include time-out, two were missing dates, and 122 were missing badge ID numbers. The Lottery Security Procedures Manual states that Lottery employees will assist visitors in filling out the log, and will record the outgoing time if the visitor forgets. Although the Lottery Security Procedures Manual states, "The desire is that the logs be filled out as completely as is reasonably possible," at an average of less than two visitors per day, it is reasonable to expect that log entries will be complete. We also reviewed entries to the warehouse visitor log for calendar year 2005. Of the 248 entries reviewed, two were missing the date, six were missing the time-in, six were missing a name, 17 were missing the time-out, and six were missing the reason for entry. By not ensuring visitor logs are complete, the Lottery cannot effectively demonstrate that internal procedures are being followed to ensure accountability if a breach of security were to happen on the Lottery premises or in the warehouse.

Recommendation #8

We recommend the Lottery ensure Lottery premises and warehouse visitor logs follow the documentation requirements outlined in the Security Procedures Manual.

Electronic Access to Lottery Premises

To ensure security of the Lottery premises and warehouse in accordance with section 23-7-411(k), MCA, the Lottery has documented procedures established to allow employees and

Chapter II - Findings and Recommendations

contractors physical access through the use of electronic key cards. Additionally, an electronic alarm system is used that can be activated and deactivated using a key code. The procedures state that key card access will be controlled to ensure employee access is appropriate for their job function. Procedures also state that alarm key codes should be changed periodically as employee turnover requires it.

Key Card Access for Contractors Not Controlled

We reviewed key card access for employees and contractors. We identified four contractor key cards that allowed access seven days a week. The contractors only required key card access two of the days, and currently have a level greater than what is appropriate for their job function. For example, the contractors only need access on Wednesdays and Saturdays, but have access every day of the week. After follow-up, we determined that because of a system limitation, key card access can only be assigned for either five days a week (weekdays) or seven days a week, and that the new system they plan to implement will have further capabilities. We identified a generic key card assigned to a 'group' of contractor employees. Lottery security personnel stated that the contractor is a new contractor, and was given the card initially because they did not know who all needed access. The Lottery cannot ensure individual accountability of personnel accessing the Lottery premises through the use of a generic key card. The key card access system logs which key cards are accessing which doors, and when. By sharing the key cards, it is not possible to determine through the logging, who is using the key card.

Recommendation #9

We recommend the Lottery:

- A. Ensure key card access is restricted to time periods necessary for job requirements.**
- B. Discontinue the use of generic key card access.**

Montana Lottery Response

Montana Lottery

February 23, 2006

RECEIVED

FEB 23 2006

LEGISLATIVE AUDIT DIV.

Ms. Tori Hunthausen
Deputy Legislative Auditor
Information Services and Operations
Office of the Legislative Auditor
State Capitol Building
Helena, MT 59620-1705

Subject: Response to Montana Lottery Security Audit

Dear Ms. Hunthausen:

Thank you for the opportunity to respond to the report on Montana Lottery Security.

The Montana Lottery concurs with the audit findings and recommendations. We will take the necessary action to comply with all recommendations.

The following is our response to specific recommendations of our audit team.

RECOMMENDATION #1

We recommend the Lottery:

- A. Discontinue the use of the default administrative account.**
- B. Comply with MUSL standards and ensure the 'least privilege' security model is followed for the computer gaming system and game management system.**
- C. Establish procedures to periodically review contractor access privileges.**

We concur and will implement changes in response to this recommendation. The Director has determined that the Lottery Security Director will assume responsibilities for monitoring compliance within these areas.

RECOMMENDATION #2

We recommend the Lottery:

- A. Comply with MUSL requirements to run the secondary computer gaming system as the primary computer gaming system during a minimum of one draw period on a semi annual schedule.**
- B. Ensure contractors are aware of MUSL requirements.**

We concur and will implement changes in response to this recommendation. The new Gaming system vendor's contract starting on March 30, 2006, contains requirements that they remain in



compliance with MUSL standards and allow oversight of operations by Lottery personnel. Procedures will be in place by April 15, 2006 for semi-annual fault over testing of the new primary and backup systems.

RECOMMENDATION #3

We recommend the Lottery comply with MUSL standards to review firewall configurations on a semi-annual basis.

We concur and have implemented changes in response to this recommendation. Procedures are now in place.

RECOMMENDATION #4

We recommend the Lottery:

- A. Comply with password change policies to change passwords every sixty days.**
- B. Eliminate all but one contractor internal control system account.**

We concur and have implemented changes in response to this recommendation. Procedures are now in place.

RECOMMENDATION #5

We recommend the Lottery comply with MUSL standards to ensure contractor access requests and maintenance and changes to the internal control system are documented.

We concur and have implemented changes in response to this recommendation. Procedures are now in place.

RECOMMENDATION #6

We recommend the Lottery:

- A. Establish patch management procedures for the systems under its operation, including the computer gaming system and internal control system.**
- B. Ensure desktop machines are patched in accordance with statewide IT policy.**

We concur and have implemented changes in response to this recommendation. Procedures will be in place for all Lottery operations by April 15.

RECOMMENDATION #7

We recommend the Lottery comply with internal security investigations procedures and ensure files for all employees and contractors are maintained, containing necessary documentation.

We concur and have updated files in response to this recommendation. Done and new procedures are now in place.

RECOMMENDATION #8

We recommend the Lottery ensure Lottery premises and warehouse visitor logs follow the documentation requirements outlined in the Security Procedures Manual.

We concur and have informed all employees that any visitor must fill out the logs completely. Done and new procedures are now in place.

RECOMMENDATION #9

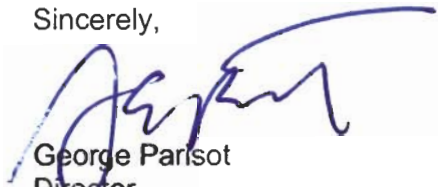
We recommend the Lottery:

- A. Ensure key card access to time periods necessary for job requirements.**
- B. Discontinue the use of generic key card access.**

We concur and have implemented policy changes in response to this recommendation. A new electronic security system will be in place for all Lottery operations by April 15.

Thank you, again for the opportunity to respond. Your team established a good rapport with our office and showed strong professional knowledge and personal professionalism while working in our area. Please express my appreciation of these facts to them for their efforts.

Sincerely,



George Parisot
Director
Montana Lottery